Strategy Research Project

CYBER DOMAIN EVOLVING IN CONCEPT, BUT STYMIED BY SLOW IMPLEMENTATION

BY

COLONEL MICHAEL S. SIMPSON
United States Army

USAWC CLASS OF 2010

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 MAR 2010		

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Domain Evolving in Concept, but Stymied by Slow Implementation	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Michael Simpson	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**30**	

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

USAWC STRATEGY RESEARCH PROJECT

CYBER DOMAIN EVOLVING IN CONCEPT, BUT STYMIED BY SLOW IMPLEMENTATION

by

Colonel Michael S. Simpson
United States Army

Colonel Richard J. O'Donnell
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Michael Simpson

TITLE: Cyber Domain Evolving in Concept, but Stymied by Slow Implementation

FORMAT: Strategy Research Project

DATE: 19 March 2010 WORD COUNT: 5,526 PAGES: 30

KEY TERMS: Cyberwarfare, Cyberspace, Cyber Domain, Cyberterrorism, Cyber Security, Information Operations

CLASSIFICATION: Unclassified

Government and private sector cyber experts have been tackling challenges in the cyber domain for the past twelve years. An evolving concept is clearly starting to take shape, but is hindered by an unsynchronized focus and a failure to integrate this potential from both an offensive and defensive perspective. To truly realize the potential of the cyber domain, the U.S. must develop more robust strategies which can evolve at the speed of technology, policies, and laws which can be feasibly implemented, and an integrated structure led by a single organization charged with providing clear vision and focus. In short, in order for the U.S. to be successful in the cyber domain of the future, it must put forth effort, resources and vision similar to those of air, land and sea domains.

CYBER DOMAIN EVOLVING IN CONCEPT, BUT STYMIED BY SLOW IMPLEMENTATION

As background, warfare that incorporated complex capabilities beyond just blunt force was predominately fought between nations and state actors. Since World War II, however, non-state actors have integrated advanced capabilities to seek asymmetric advantages over larger rival state actors. Recently, these capabilities are becoming increasingly reliant on cyberspace. As a result, the degree to which cyberwarfare's role will affect the future given the global interdependency of networks and cost effectiveness of a relatively inexpensive use of force, has been debated.[1] Former Deputy Secretary of Defense John Hamre testified to Congress in 2000 regarding cyberspace that "you can basically say we are at war"[2] Recently, Deputy Defense Secretary William Lynn warned that cyber threat options "appeal to foes who are unable to match the U.S.'s conventional military might."[3]

The challenge of defining cyberwarfare is a blurred divide between teenage cyber pranks and attacks by state and non-state actors, as well as an ambiguous oversight among non-Department of Defense (DOD) policies, strategies, and organizations. With the advances in cyber technology and virtual global reach, nearly anyone with cyber connectivity can instigate conflict in cyberspace. As such, aspects of cyber must now be considered/accounted for and incorporated in every facet of today's warfare planning at every level from tactical to strategic. The Department of Defense and the Interagency need to embrace the fact that cyberspace can no longer be treated as just another extraneous factor. It must plan, organize and execute

cyberspace operations with a focus similar to air, land and sea domain operations throughout the entire spectrum of conflict from irregular to conventional warfare.[4]

To understand the unsynchronized and stymied implementation within cyber, it is important to understand the domain's evolution. William Gibson is sometimes credited with inventing or popularizing the term by using it in his novel of 1984, *Neuromancer*[5]. Cyberspace is a relatively new domain to the DOD and, as such, understanding the implications of cyberwarfare are continually evolving. Cyber, however has been evolving globally for some time at a rate that includes technical advances doubling every couple of years.[6] According to Congress, "cyberspace is the total interconnectedness of human begins through computers and telecommunication without regard to physical geography."[7] "National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) defines cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people."[8] These definitions accurately describe cyber from a defensive perspective, but do not reflect the speed of technology, need for unity of effort, nor the ability to strike first in a cyber war.

The most telling characteristic of cyber is that it has evolved without the advantage of time, theory, and pontification afforded to the other domains. This combined with the quick rise in sophistication and application in war has helped create a flurry of unsynchronized efforts within the domain. Complicating the speed of cyber application is that cyber threats have evolved commensurate with the speed of cyber

technologies. The exponential growth of cyber interest and technologies has complicated common understanding and limited synchronization across the government and private sectors. DOD was the first government agency to recognize cyber as a domain and changed its definition in 2008 to “a global domain within the information environment consisting of the interdependent network of information technology infrastructures including the Internet, telecommunications, networks, computer systems, and embedded processors and controllers.”[9] This definition implies DOD still mixes cyber with other information operations and that cyber does not have a unique identity and is not on par with other domains. Moreover, a lack of a common cyber understanding has attributed to ineffective U.S. policy and fostered a culture that exhibits a cautious use of offensive cyberwarfare. This lack of unity and synchronization for comprehensive and coordinated cyber policy has hampered the U.S. military’s ability to exploit more robust cyberwarfare operations.

Gaps still remain in the refinement of the cyber domain understanding and its operating boundaries such as private, public, international and war environments. The convergence of cyber and terrorism spawned a following of academics that argue cyberterrorism should receive distinctive recognition in cyberspace. “It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political objectives.” [10]

In 1998 the military enhanced the cyberspace unity of effort with the formalization of a Computer Network Operations (CNO) mission that assigned U.S. Strategic Command as a means to begin create an advocate for material and roles. While this

organizational change provided an advocate for CNO, lack of synchronized action has caused policies and procedures to still remained underdeveloped. Twelve years later the domain has been molded as noted in figure one below into disparate pieces and parts in need of integration.

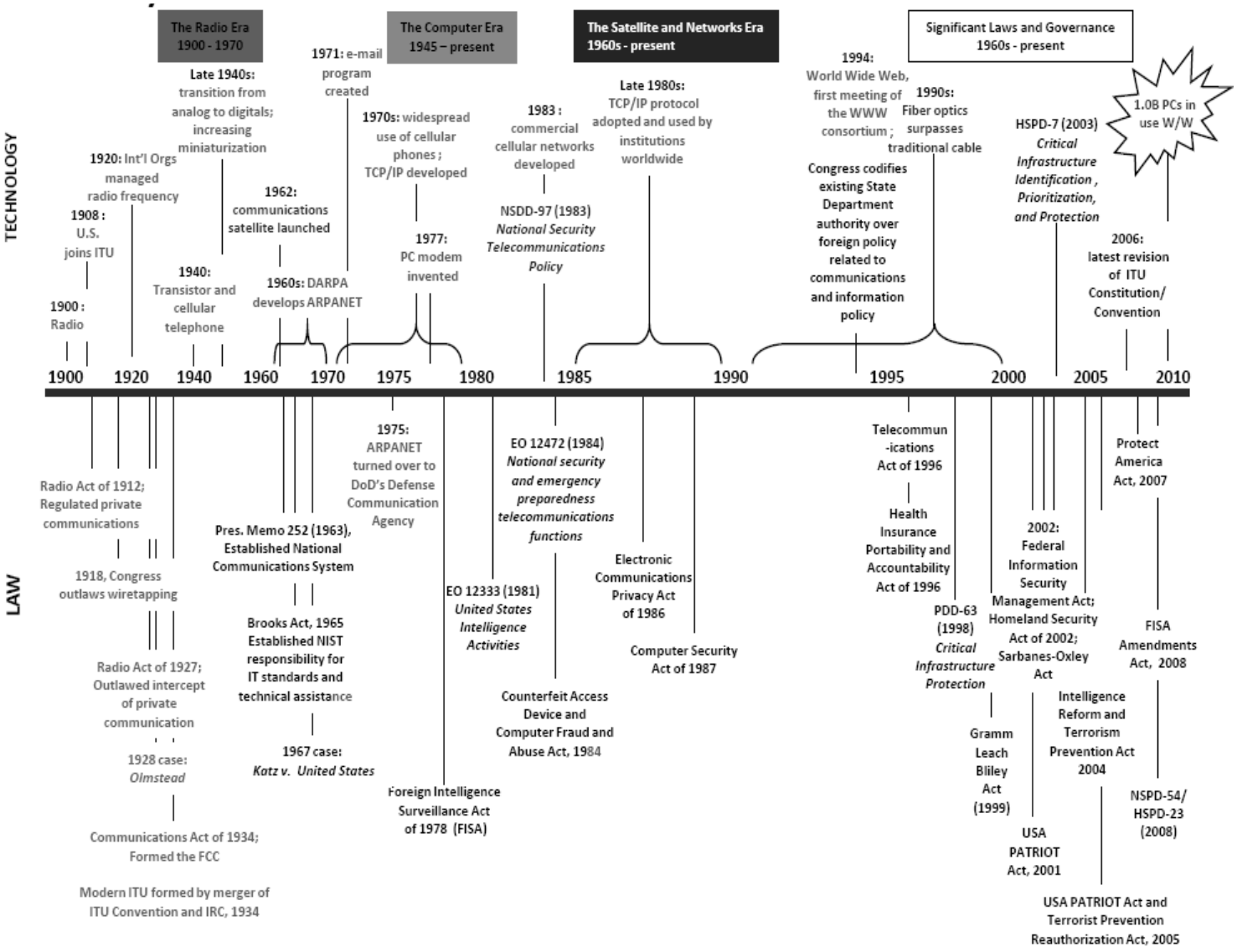

Figure 1[11]

As this research project was initiated, it was hypothesized that this relatively new domain was dysfunctional and ungoverned. A more refined premise is that the U.S. government has made recent strides but still wrestles with many areas for improvement. A lack of integration, execution and awareness are all factors key to the understanding of on-going progress. As such, this new domain is no longer dysfunctional, but rather, disjointed. Moreover, the cyber domain's governing principles exist, but are outdated. The reasons for the lack of understanding are many. Key among them are outdated governing principles, a non- integrated governmental approach, and a noticeable lack of focus and planning for offensive operations.

In the past year, there are four achievements that highlight advancements in cyberwarfare thinking, but most of these initiatives are still hampered by ineffective implementation strategies. First is the Comprehensive National Cybersecurity Initiative (March 2009) that noted antiquated governing legal authorities and policies and identified need for change.[12] Second was the Cyberspace Policy Review (April 2009) which provided an interagency critique of current cyber policy that noted gaps and seams in structure, execution and policy.[13] Third was the December 2009 appointment of a cyber-czar for the President in hopes that cyber issues would gain greater prominence.[14] The fourth advancement was recent military advances in cyber including raising the level of cyber importance in the 2010 Quadrennial Defense Review (QDR) and the creation of U.S. Cyber Command which includes a reported offensive engagement strategy.[15] While these achievements are noteworthy, most of the recommendations and implementation are still pending.

The slow pace of transferring concept to action has created a lack of common understanding of the current status of U.S. cyber policy, structure processes and execution. Weak or non-existent implementation has limited the evolution of cyber concepts and exasperated the ambiguous identity of cyber over the past ten years. For instance, in the beginning, the tech boom in 1999-2000 reflected the still fledgling cyberspace before its emergence as a domain. Then, the terrorist attack on the U.S. on September 11, 2001, reemphasized the need to move faster operationally, be alert defensively, and seek opportunities for exploiting cyber advances. Despite its early existence and 2001 highlight as an emerging priority, computer network operations (CNO) still went relatively unnoticed. Since 2005, emerging threats, policies and the establishment of a formal domain have re-energized momentum. This paper will endeavor to highlight areas where progress can be achieved in policy, law, planning, and organizational structures. Recommendations will be provided which address organizational synchronization that focuses more on the need for active engagement rather than passive or defense cyberspace effort. Finally, recommendations will be provided which reflect the need to incorporate cyber planning across a broader range, bringing it more on par with the way we treat the other domains of air, land and sea.

Policy

Prior to 2008, our national strategies infrequently addressed cyberspace, cybersecurity, and cyberwarfare. Since 2008, some progress has been made in the policy and strategy arena as previously noted (Figure 1). However, most of this progress was associated with cybersecurity. The 1998 Presidential Decision Directive (PDD) 63 on Critical Infrastructure Protection[16] and the Homeland Security Presidential Directive 7 (HSPD-7) which superseded PDD 63 and gave responsibility of critical

infrastructure to the Department of Homeland Security and are two key examples of this focus.[17] Global threats and attacks have risen awareness of a need for defensive measures that have unfortunately overshadowed the need for offensive strategies. This was highlighted in the 2003 Bush Administration National Strategy to Secure Cyberspace focusing on the defense and limitations created by privacy and civil liberties issues.[18] There are still gaps and a lack of synchronization in all if these areas.

The first signs of offensive operations to be considered as part of U.S. strategy was the National Military Strategy for Cyberspace Operations (December 2006) that called for dominance and strategic superiority in cyberspace.[19] Due to emerging threats and a rise in global network attacks, defensive strategies on cybersecurity continued to dominate cyber policy and initiatives. A positive ray of hope yet to be exploited is the February 2010 release of the Quadrennial Defense Review (QDR). This QDR stresses new threats such as cyberwar and lists a "plan for a wide spectrum conflict in cyberspace" as one of the Pentagon's four goals.[20] This has not yet been fully translated into action nor has it been fully funded. The National Defense Strategy 2008 states the defense of the homeland (as based in the Quadrennial Defense Review 2006) must include support to defend cyberspace against attack, but espouses the Department of Defense as a supporting role to the Department of Homeland Security (DHS) and only emphasizes its role through deterrence.[21] Cyber is marginally mentioned in the Department of State Strategic Plan 2007-2012 (crime and infrastructure), DHS Strategic Plan 2008-2013, and National Security Strategy (NSS 2006), but not at all mentioned in the Office of the Director of National Intelligence (ODNI) Strategic Intent 2007 nor the ODNI 2007 500 Day Plan.[22]

Background documents above show a lack of unified national policy as part of the cyber strategy formulation which has been hampered by the limited evolution of specific theory (the closest comparison is often nuclear warfare) as noted earlier.[23] Moreover, in the development of the cyberspace understanding, enduring beliefs, ethics and values have been largely ignored or, where there is conflict, have not been resolved. For instance, the quandary of personal privacy and legalities has contrasted the need for freedoms, economics, and personal liberties as noted in the Posse Comitatus Act (PCA). [24] The conservative nature of personal liberties are also denoted in the limitations of the much contested Patriot Act which was due to lose many of its provisions but received a temporary extension until the end of February 2010.[25] As such, U.S. strategy formulation, which should serve as a foundation for U.S. policy, aligned to national interests without sorting out differences in national purpose, nor having a basis of understanding via an established theory. The evolution of the policies and legal cyber collection/monitoring were watered down to meet implementing feasibility standards and have resulted in reactive initiatives which are not suitable for the exponential threat evolving in cyberspace creating a reactive chain of modifications rather than a grand proactive approach. This has contributed to the lack of synchronized strategy among agencies and a misdirected assignment of ODNI for a lead review of cyber, and a DOD strategy that relegates its role in support to DHS.

Another shortfall in our national and interagency policies is the need for a cyberwarfare offensive first strike option. Our current U.S. policy cyber objectives are to enhance or improve cybersecurity. Moreover, it is to understand, detect, and counter adversary threats to enable protection of the Nation's information infrastructure.[26]

Stated efforts are: leverage partnerships; protect infrastructure; reduce vulnerabilities; combat cyber threats to non-traditional targets; manage cyber mission processes.[27]

A bright spot in recent policy developments is the completion of the National Cyberspace Policy Review. According to the 60-day review by cyber experts, the nation is at a crossroads, the status quo is not acceptable, and national dialogue must begin today in an open forum free of government isolation. [28] A summary of a near- term action plan is centered around renewed emphasis on strategy, organization and laws as depicted in figure 2.[29]

NEAR-TERM ACTION PLAN	
1.	Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2.	Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3.	Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
4.	Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5.	Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.
6.	Initiate a national public awareness and education campaign to promote cybersecurity.
7.	Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8.	Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement
9.	In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
10.	Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

Figure 2

The ideal recommendation is to immediately garner support, implement, fund, and create metrics against the near-term action plan noted above. For a long-term solution, our founding strategy documents for all members of the Interagency need to adequately address cyber as a priority from the top down. Moreover, funding needs to be procured as a priority for long-term investments in technological advances and supporting organizations. Secondly, once cyber strategies and policies are updated, the next challenge will then be to incorporate them among vast public and private cyber domain related organizations. Once the private and public sectors are synchronized, the next recommendation would then be to review and establish policies to divide authorities over the different cyber domains such as .mil, .gov and .com. Currently, the military operates and protects .mil, DHS engages .gov, and there is not a designated private sector lead for .com.[30] This lack of integration hinders the ability to share information and clearly identify proper authorities. As will be noted later, the creation of a new departmental-level structure is well suited for this function. Lastly, our policies need to be feasible in accordance with the laws and ethics that govern cyber domain operations.

Law and Ethics

Conservative laws and ethics surrounding cyber impede the implementation of robust cyber policies and operations . Although the United States has an enormous cyber information capacity, its cyber influence is not proportional to that capacity in large part due to legal regime limitations.[31] U.S. persons are constitutionally constrained. Although the laws have been identified as problems in the past, complacency and the lack of cultural development have blocked actions to update the laws. Admiral Blair testified before congress that sensitivity toward U.S. person's privacy limited proactive

options that could have deterred or denied the “Christmas 2009 bomber” from initiating what was fortunately a failed attempt to bring down a U.S. airliner in flight. This is also a similar possible flaw in the prevention of the Fort Hood 2009 shooting. [32] Possible SAEDA tips, even if reported, would have likely faced scrutiny when evaluated based on the restrictive nature of the Foreign Intelligence Surveillance Act of 1978. [33] The suspected use by terrorists of steganoghy in the 9-11 attacks also highlights the challenges of technology’s ability to outpace the flexibility of laws designed to balance the need for successful cybersecurity and cyberwarfare with concern for civil liberties and privacy.[34] Complicating cyber freedom of action are conservative administration officials such as the newly appointed Cyber-Czar for President Obama who stated that he does not support the use of monitoring private sector networks or internet traffic.[35]

How can the U.S. practice and demonstrate capability (to deter) without breaking laws (in peacetime settings)? Regardless of the element of power being considered, a cultural maturation is required. Cyberwarfare must be considered as an act of war in both planning and policy so we can deny sanctuary to threats in cyberspace.[36] There is a need for a more liberal use of intelligence oversight that guides intelligence cyber operations. AR 381-1 (U.S. Army Intelligence Activities; 2007, the Army’s authority on intelligence oversight) and similar other service component documents are badly in need of updating. These concerns are not unique to the U.S., similar legal challenges hamper European Union (EU) nations due to the Charter of Fundamental Rights of the EU to provide data protection and ‘constitutionalization’ of individuals.[37]

Information Sharing Rules

Noting that there are international and interagency members of the cyber domain emphasizes the need for more liberal information sharing laws and rules to ensure

successful multilateral operations. Since cyber is a global domain with virtual tentacles across national boundaries, the laws governing collaboration must match or exceed the enemy's ability to outmaneuver friendly operations. Currently, international information sharing for instance is limited through Mutual Legal Assistance in Criminal Matters Threats (MLATS). There are currently only nineteen international agreements between the U.S. State Department which are monitored for action by the FBI Legal Attaches (LEGATS) for international authority.[38] The role of information sharing needs to expand more globally to include non-criminal matters and bring cyber domain on par with other agreements.

To remove the mystery and lack of legitimacy that creates the barriers in cyber's legal regime, the U.S. strategy needs to declare our cyber domain capability and overcome the secrecy surrounding the technology. This includes allowing intelligence and operations units to co-exist in a ways that current laws do not allow. Cyber attacks and security require a great degree of collection and collaboration. Currently, this capability is hampered by disparate data systems, conservative collection authorities, and organizational challenges. The House and Senate Intelligence Committees have called for greater clarity "in the kinds of cyber operations under consideration and for improved coordination between the Pentagon, CIA and FBI to keep their hackers from tripping over one another" in cyberspace.[39] A tremendous advantage of an interagency cyberspace organization would be the ability to seek legal collaboration on collection. Common interagency databases are still not required and Intelligence Oversight laws still restrict timely collection on US persons. Within a network of cyber domain agencies is a need for a Google-like capability in the intelligence community. The worth of this

data will be measured by its depth across the government and private sector, as well as input from the international community through robust international agreements. Although these agreements may reveal some closely guarded U.S. techniques, procedures, and tradecraft, it is time to employ global assets to conquer a global threat. This would include sharing nationally and internationally among the many Computer Emergency Response Teams (CERTS).[40]

The boundaries of public and private sector networks, complicates the ability to reform the cyber domain laws and ethics to allow for comprehensive and integrated operations. Matched with an expanded planning strategy and a more synergized organizational structure, the U.S. would be better prepared to meet the need for the challenges on cyber to ensure aggressors do not achieve strategic or technical advantages. Once all the laws are adjusted to match updated policy and strategy, planning could be more robust and unilaterally integrated across the Interagency.

Planning

The integration of cyber into the planning process is another significant area of concern. In the military planning models, cyber is generally considered a subset of information operations. Cyberspace lacks the same distinctive planning emphasis as other domains such as land, sea and air.[41] Currently, cyber operations are typically discussed in annexes or as a defensive measure related to operations security (OPSEC) or another measure requiring mitigation. STRATCOM for example, buries cyber (stated as CNO) under Information Operations as one of five pillars on par with lesser enablers as OPSEC which is validated under Joint Publication 3-13 Information Operations.[42] Cyber planning needs to be embedded throughout the planning process and not fall into obscurity in the way that interagency planning was isolated by PDD 56

as Annex V of the Joint Planning Doctrine.[43] This document clearly segments elements of planning into stove-piped areas versus integrating across the entire spectrum of the plan from concept, through execution, to endstate. This lack of parity when compared to other domains is especially noticeable in the formulation of offensive doctrine. The planning processes associated with cyber should be more closely aligned with the other domains (land, air and sea) which routinely encompass domain considerations throughout the entire planning process.

Complicating the planning of cyber is that the Department of State only recently created a documented planning process and the Department of Homeland Security's formal planning process is still under development. Neither are known to have highlighted cyber as a focus area nor addressed integrated planning across the interagency.

Cyberspace operations also needs a separate and distinct planning consideration (i.e. its own paragraph) throughout the entire planning process and subsequent documents. According to General Alexander, Cyber Command Commander, revised joint doctrine is needed to expand on cyberspace operations and might include breaking cyber out from JP 3-13 into its own Joint Publication.[44] Revising doctrine and creating a unique cyber publication would go a long ways toward synchronizing and integrating cyber throughout the entire planning process and the documents that come out of that process.

As part of the planning factors and risk mitigation, another doctrinal adaption is the need to expand the Force Protection Condition (FPCON) criteria into the cyber

domain with its own designator such as Cyber Condition (CyberCon) to bring it on par with the importance of other warning criteria.

Offensive Planning

No review of feasible cyber planning implementation would be complete without incorporating the aspects of offensive and defensive operations. Over the past decade, cyber has focused on defense and discussions of offensive planned operations have been commonly dismissed as too hard. The U.S. must develop and implement offensive strategy and planned operations to help maintain the strategic, operational and tactical advantage over adversaries who are not shy about using all methods of available cyber. In many conflicts, it is often said that the best defense is a good offense. Sun Tzu highlighted the need for proactive engagement of attacking the enemy's strategy.[45] For planning purposes, we are still in reaction mode when it comes to cyberspace. Recent DOD operations reflecting potential expansion beyond the use of defense are: Burnt Frost (shoot down of satellite), STRATCOM's Countering Adversarial Use of the Internet (CAUI) and Buckshot Yankee (efforts to counter adversary/virus in networks). [46] The government has yet to fully adapt to the Bush doctrine of cyber "first strike" and integrate it as an interagency tool of power. Arguably this can be attributed to the cyberspace designation as a relatively new domain that is trying to define itself. Current definitions of attack in cyberspace are ill-defined for areas like espionage versus denial of service. For offensive operations to be successful, it is critical to be able to target an attributable threat. This capability was highlighted when Russia, with little warning, attacked Georgia allegedly using offensive cyber denial of service as a hard power tactic difficult to trace back to Russia but

demonstrating Russia's willingness to integrate cyber into offensive operations in cyberspace.[47]

The lack of warning from threats in cyberspace differ from traditional warning factors of conventional weapons and highlight even more the importance of offensive planning.[48] Nations such as China and Russia are developing their own cyberspace warriors including battalions and regiments trained to find and exploit weaknesses in military, government and commercial networks undetected at nano second speed. Russia, for instance, believes "the danger of cyberwarfare ranks second only to that of nuclear war".[49] Robust threat capability enhances their ability for tactical surprise and use swarming which is "a seemingly amorphous, but is deliberately structured, coordinated, strategic way to strike from all directions at a particular point or points using dispersed nodes of a network of forces which is difficult to defend against."[50] For cyber threats it is said if a threat can be detected, it can be defended. If it can be defended, it can be defeated, thus reducing the requirement for a defense in the first place. Secretary of State Hillary Clinton has communicated this requirement when she stated "countries or individuals that engage in cyber attacks should face consequences and international condemnation."[51]

Many experts agree that creating a policy in which offensive and defensive operations work together is badly needed, but struggle to find the balance between privacy and security and worry about differentiating between enemy network attacks and accidental factors like friendly implementation mistakes. The new Cyber Command is reportedly working on classified offensive operational capabilities , but its secrecy has created concern about effectiveness and oversight toward civil liberties.[52] "We have

U.S. warriors in cyberspace that are deployed overseas and live in adversary networks"[53] According to General Alexander, new Cyber Command Commander, " the only way to counteract both criminal and espionage activity online is to be proactive."[54] This requires getting ahead of botnets (a cluster of many compromised or offensive cyber assets launched with a master control within networks) involved in recent attacks in South Korea, Estonia (07) Georgia (08), and U.S. government sites. A basic premise of attack is the need to attribute the legitimacy of the offensive to an adversary. "The internet provides terrorists with anonymity, command and control resources, and a host of other measures to coordinate and integrate attack options".[55] Non-state actors and terrorist pose some of the greatest threat due to the cyber "safehavens" created by the ability to divert or hide the true origins of cyber networking.[56] To combat cyberterrorism is not without complications regarding laws and ethics protecting innocent civilians sharing the same domain space and will require a sophisticated collection and global information sharing process, the development of socially acceptable collection and analysis, and the full integration of offensive capability into hard and soft power.

Structures

The gaps and lack of implementation of cyber concepts is partly due to a disparate and disjointed multi-organization domain fueling a stalled strategic unity of effort. Cyber organizational structures need to be adjusted from the top down to optimize effectiveness. The concepts have been evolving, but are not yet fully implemented. Most recently, President Obama verbally stated cyber as a priority (the next NSS is not yet published) and in February 2009 directed a cyber interagency review/study led by ODNI. Ironically, cyber in the Executive Branch was until recently the President's Assistant for Homeland Security and Counterterrorism, John Brennan.

In December 2009, nearly seven months after President Obama vowed to make cybersecurity a priority, he named Mr. Howard Schmidt as his new cybersecurity advisor. There is still debate on how much authority this new "cyber-czar" will have.[57] Howard Schmidt, formerly of Microsoft and a previous cybersecurity advisor for the Bush administration, leads a cyber office that focuses more on security ("government strategy for protecting computer systems") and ignores full spectrum interagency/international operations, but does include links to the Office of Management and Budget on funding allocated for cybersecurity priority purposes.[58] Schmidt left his advisor position with the Bush administration reportedly "out of frustration that the government wasn't making cybersecurity a priority." In concert with the President's emphasis, National Intelligence Strategy 2009 added a mission objective for enhancing cybersecurity, and DOD established Cyber Command.[59] Many elements of the Department of Justice, especially the Federal Bureau of Investigations (FBI) have built cyber entities, but, as is the case of our national and interagency policies, these organizations are not linked and the law enforcement and intelligence communities are prohibited from virtual connections to each other. An example is the Law Enforcement Counterintelligence Center (LECIC) which is an FBI-led multi-agency within DOD's Joint Task Force Global Network Operations (JTF-GNO) at the Defense Information Systems Agency (DISA).[60] At the LECIC, multiple DOD and Department of Justice agencies share a common workspace, but each maintains its own database which is not available to each other. Instead of a common database in which virtual connections are available, the agency relies solely on over-the-shoulder monitoring as a means of sharing. Most organizations have created Task Forces and assigned liaisons between

each other such as NSAs National Threat Operations Center (NTOC), but these relationships tend to be adhoc and fraught with gaps and seams, and lack a unified authority that spans all aspects of computer network operations, including offense.

The disjointed government organizations have caused inefficient cyberspace management and consistently create gaps in conceptual implementation. A possible recommendation, though daunting, would be to create an additional interagency department in the government that is dedicated to cyber so it is not relegated as a secondary issue in other departments. This arrangement would allow a singular focus and eliminate the ongoing relegation of cyber considerations that are prevalent in many of the departments. The creation of such a department, that could be called the Department of Cyber and Communications, would clear any confusion as to who has the lead and would be best postured to synchronize cyber activities. The next step should then be to assign the new department secretary as the lead for the President's review/assessment of cyber policy. A better monitoring process orchestrated at the department level could also entice/mandate industry to report cyber vulnerabilities (current industry practice is to withhold cyber attacks for fear it would reflect negatively on the company and created a competitive disadvantage). The current Executive Branch representative does not have operational authority. A cabinet-level department agency is the optimum recommendation and would tie government organizations together as well as bridge private and public cyber alliances.

A new department as described above would help settle disputed authorities between DHS and the FBI's Joint Terrorism Task Forces (JTTF) and their Counterintelligence/counterterrorism Investigations Unit (C3IU). The current

suborganizations in DOD would still link to Cyber Command who would then connect to the next echelon at the Department level and be able to leverage this linkage as an advocate for cyber priorities and deconfliction of operations and legal challenges. The suborganizations within DOD include each Service organization which need their own updated implementations as well as integration.

Service Cyber Structure Efforts

As much as the interagency has a disjointed cyber effort, the military is not much better at integrating cyber mission statements and corresponding objectives. The Navy and Air Force have begun transforming concept into reality, but the Army is lacking a way forward. With that said, all services still lack integration among each other. For DOD, Cyber Command was created for this purpose. Parallel to Cyber Command at a training and laboratory level is the Defense Cyber Crime Center (DC3) which competes with the services for priority and funding creating an even wider gap toward full Service integration. Both Cyber Command and DC3 are headquarters elements with few actual operational elements. Below Cyber Command, there still remains a service (Army, Navy, Air Force, and Marine) issue where collaboration, deconfliction and execution are still adhoc. The Air Force has been the most active to create a formal cyber organization called the 24th Air Wing and added cyber into its service mission statement.[61] The Navy has designated 10th Fleet for its lead on cyberspace. The Army lacks a similar structure to enhance cyber operations and more readily facility integration into planning and execution with Service operations, training, and doctrine. The Intelligence and Security Command's attempts to create an Army unit were fraught with legal (for offensive operations) and doctrinal issues, and consequently never matured. The Signal community is the latest to develop an Army unique structure to

deal with the cyber domain, but they are defensive in nature. With the Air Force as an example, each service should create a unit that can collaborate with Cyber Command.

Each service has distinct considerations needed for legitimacy such as skill qualifications and identifiers (for the Army that translates to a Military Occupational Specialty – MOS). Natural progression from a personnel structure is a training base, with corresponding funding and equipping. Without formal cyber professionals, the highly specialized training is often short lived due to the competitive nature the private sector has to offer. Moreover without cultural savvy and technical specialist dedicated to this mission, cyber organizations quickly loose legitimacy within DOD.[62] To compensate for personnel training and shortfall, the less-than-optimal DOD fix for those designated with the task of working cyber has been to pull from the communications, criminal forensics, or information operations branches. These areas, though similar, do not offer the same qualifications.

Successful cyberwarfare operations must be built from the Service level. Cyber can no longer be solely thought of as a soft power. In the military sense, it can and should be considered as a kinetic tool of military force. Once the disjointed structures of DOD and the rest of the government are resolved, the ability to effectively plan and efficiently conduct interagency operations will be possible.

Conclusion

As demonstrated throughout this paper, government and private sector cyber experts have been tackling challenges in the cyber domain for the past twelve years. Their efforts, however, have failed to clearly communicate the challenge, synchronize the efforts, and to keep up with technology and global threats. More importantly, many concepts have not evolved into action. Given the degree that adversaries are operating

in cyberspace, the need to act fast is now at crisis levels. It is time to create more robust strategies, liberal policy and law, synergistic plans that include offense and defense, and an integrated interagency and private sector structure with defined leadership at the top. These components need to be enabled with a new emphasis on the military's ability to deliver kinetic cyber blows using international and interagency linkages to discover and defeat state and non-state actors. The military structure should include a professional force trained and culturally savvy in the cyber domain that can create a warning mechanism and provide an offensive capability. Cyber planning processes should be implemented on par other domains vice buried deep in the bowls of information operations. Disjointed, ineffective structures and outdated policy must be transformed and given an expanded range of authority if we are to ensure cyber dominance in the future.

Endnotes

[1] Timothy Shimeall, Phil Williams and Casey Dunlevy, "Countering Cyber War," *NATO Review* no. 49 (Winter 2001/2002):16

[2] Steven A. Hildreth, "Cyberwarfare" *Congressional Research Service Report for Congress* (November 15, 2001): 1

[3] Mark Thompson, "U.S. Cyberwar Strategy: The Pentagon Plans To Attack," February 2, 2010, http://ebird.osd.mil/ebfiles/e20100203732204 (accessed February 3, 2010).

[4] Richard Mereand, "Securing Cyberspace: Guarding the New Frontier," Association of the U.S. Army National Security Watch, no.3 (24 August 2009): 4.

[5] Ibid.

[6] Steven Hildreth, "Cyberwarfare", *Congressional Research Service (CRS) Report for Congress*, (Washington, DC: U.S. Government Printing Office, November 15, 2000; updated June 19, 2001), CRS-1.

[7] Ibid.

[8] Cybersecurity Office, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC, White House, April 2009), 1.

[9] Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, 12 April 2001 (as amended through 31 October 2009): 139.

[10] Alan O'Day, *Cyberterrorism* (Vermont: Asgate, 2004), xi.

[11] *Cyberspace Policy Review*, C-13.

[12] John Rollins and Anna C. Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations," *Congressional Research Service (CRS) Report for Congress*, (Washington, DC: U.S. Government Printing Office, March 10, 2009), 1.

[13] *Cyberspace Policy Review*, iii.

[14] Ellen Nakashima, "Obama Set to Create A Cybersecurity Czar With Broad Mandate: Shielding Public, Private Networks Is Goal," *The Washington Post*, May 26, 2009.

[15] Mark Thompson, "U.S. Cyberwar Strategy: The Pentagon Plans To Attack," February 2, 2010, http://ebird.osd.mil/ebfiles/e20100203732204 (accessed February 3, 2010).

[16] Presidential Decision Directive (PDD)/NSC- 63, Critical Infrastructure Protection, May 22, 1998, Sec. II, 2.

[17] Homeland Security Presidential Directive (HSPD)- 7, December 17, 2003, Policy, (7)(a)-(f), 2-3.

[18] George W. Bush, The *National Security Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003), viii.

[19] Peter M. Pace, National *Military Strategy for Cyberspace Operations,* December 2006

[20] Nancy A. Youssef, "Pentagon Review, Budget Stress New Threats Such as Cyberwar," *McClatchy Newpapers*, February 1, 2010.

[21] Robert M. Gates, *National Defense Strategy* (Washington, DC: Pentagon, June 2008), 7.

[22] George W. Bush, *The National Security Strategy* (Washington, DC: The White House, March 2006).

[23] Mike McConnell, "To win the cyber-war, look to the Cold War," *The Washington Post*, February 28, 2010.

[24] Title 18 U.S. Code, Sec 1385, *Posse Comitatus Act* (1994).

[25] U*.S. Patriot Act of 2001*, HR 3162, 107th Congress., 1st session. (October 24, 2001), Title I-X.

[26] Dennis C. Blair, *The National Intelligence Strategy* (Washington, DC; Office of the Director of National Intelligence, August 2009), 9.

[27] Ibid.

[28] *Cyberspace Policy Review*, v.

[29] Ibid., vi.

[30] Gordon Lubold, "Obama's Strategy for Countering Cyber Attacks," *The Christian Science Monitor*, May 29, 2009.

[31] Franklin D. Kramer and Larry Wentz, "Cyber Influence and International Security," *Defense Horizons*, no. 61 (January 2008): 1.

[32] Scott Wilson, Carrie Johnson and Spencer S. Hsu, "Ideology, stress or another motive?; Web postings spur questions," *The Washington Post*, November 7, 2009.

[33] The Foreign Intelligence Surveillance Act, available at http:www.usdoj.gov/usao/eousa/foia_reading_room/title9/crm01073.htm.

[34] O'Day, *Cyberterrorism*, 39.

[35] Gordon Lubold, "Obama's Strategy for Countering Cyber Attacks," *The Christian Science Monitor*, May 29, 2009.

[36] "Marching Off to Cyberwar" *The Economist* (US), (December 4, 2008).

[37] James A. Lewis, ed., *Cyber Security: Turning National Solutions into International Cooperation* (Washington DC: CSIS Press, 2003), 81.

[38] Ibid., 2.

[39] Bradley Graham, "Cyberwar: A New Weapon Awaits a Set of Rules: Military, Spy Agencies Struggle to Define Computers' Place in U.S. Arsenal," *The Washington Post*, July 8, 1998.

[40] Lewis, *Cyber Security*, 2-9.

[41] Joint Publication 5-0, Joint Operations Planning, 26 December 2006: IV19-20 (cyber not mentioned anywhere in the publication).

[42] Joint Publication 3-13, Information Operations, 13 February 2006: II-4 – II-5.

[43] Joint Publication 3-08, Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations Vol I: II-16.

[44] Keith B. Alexander, "Warfighting in Cyberspace," *Joint Forces Quarterly*, no. 46, (3rd Quarter 2007): 59.

[45] Samuel B. Griffith, *Sun Tzu The Art of War* (New York: Oxford University Press, 1971), 23.

[46] The United States Strategic Command Home Page, http://www.stratcom.mil (accessed December 5, 2009).

[47] John Markoff and Andrew E. Kramer, U.S. and Russia Differ On Treaty for Cyberspace," *The New York Times*, June 28, 2009.

[48] Timothy Shimeall; Phil Williams; Casey Dunlevy, "Countering Cyber War," *NATO Review* (Winter 2001/2002): 18.

[49] Steven Hildreth, "Cyberwarfare", *Congressional Research Service (CRS) Report for Congress*, (Washington, DC: U.S. Government Printing Office, November 15, 2000), CRS-10.

[50] John Arquilla and David Ronefeldt, eds, *Networks and Netwars: The Future of Terror, Crime and Militancy* (California: Rand, 2001), 12-13.

[51] Jack Goldsmith, "Can We Stop The Cyber Arms Race?" *The Washington Post*, February 1, 2010.

[52] Gordon Lubold, "Obama's Strategy for Countering Cyber Attacks," *The Christian Science Monitor*, May 29, 2009.

[53] Goldsmith, "Can We Stop The Cyber Arms Race?"

[54] Ibid.

[55] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of Cyberplanning," *Parameters* 33, no.1 (Spring 2003): 116

[56] George W. Bush, *National Strategy for Combating Terrorism* (Washington, DC: The White House, March 2006), 16-17.

[57] Ellen Nakashima, "Obama to Name Former Bush, Microsoft Official as Cyber-Czar," *The Washington Post*, December 22, 2009.

[58] Ibid.

[59] Richard Mereand, "Securing Cyberspace: Guarding the New Frontier," *Association of the U.S. Army National Security Watch*, no.3 (24 August 2009): 3.

[60] Law Enforcement and Counterintelligence Center (LECIC) brochure (picked up during visit to LECIC May 2007).

[61] Doug Beizer, "Air Force Cyber leader takes office," *Federal Computer Week*, June 15, 2009.

[62] Kevin P. Chilton, "Cyber Leadership: Towards New Culture, Conduct and Capabilities," Air and Space Power Journal (Fall 2009): 7.